



Masoumeh Safkhani

Associate Professor
Shahid Rajaee University

- Place of Birth:** Tehran
- Faculty of Computer Engineering, Shahid Rajaee University, Lavizan, Tehran, Iran
- +982122970117
- Safkhani[at]sru[dot]ac[dot]ir
- Scopus:** M.Safkhani
- ORCID:0000-0002-1897-0828

Languages

- Persian
- English

Interests

- Design and Cryptanalysis of Security Protocols
- Design and Cryptanalysis of Cryptography Primitives
- Network Security
- Internet of Things (IoT) Security
- Searchable Encryption Schemes Security

Profiles



Working Experience

- Sep, 2020 – ongoing **Associate Professor** Faculty of Computer Engineering, Shahid Rajaee Teacher Training University(SRTTU)
Major research area includes Design and Analysis of Security Protocols
- Sep, 2018 – March 2022 **Software Department Head** Faculty of Computer Engineering
- Nov, 2017 – ongoing **Managing Editor** Shahid Rajaee Teacher Training University(SRTTU)
in the Journal of Electrical and Computer Engineering Innovations(JECEI)
- Sep, 2014 – Sep, 2020 **Assistant Professor** Faculty of Computer Engineering, Shahid Rajaee Teacher Training University(SRTTU)
Major research area includes Design and Analysis of Security Protocols
- Fall, 2015 – Nov, 2017 **Hardware Department Head** Faculty of Computer Engineering.

Education

Postgraduate Studies

- 2008 – 2013 **Ph.D. in Electrical Engineering** IUST
Title: Design and Security Analysis of RFID protocols.
Supervisor: Prof. Majid Naderi
In PhD thesis, we investigate the security of a variety of RFID protocols and demonstrate several practical attacks against 13 RFID protocols which have recently been proposed in literature. We apply various attacks, e.g., desynchronization attack, ID disclosure attack, tag impersonation attack, reader impersonation attack or traceability attack, on those RFID protocols. In addition, in this thesis, to improve patients' safety and to decrease medications errors in e-health systems with RFID infrastructure, we proposed an RFID access control protocol and an RFID grouping proof protocol, based on symmetric cryptography. In the proposed access control protocol, not only the authentication mechanism but also the access right authorization mechanism is designed so that only the specific doctor, usually the patient's doctor, can access the patient's tag. The proposed grouping proof protocol guarantees that a collection of tags (e.g., patient's tag, nurse's tag and drug's tag) are read at the same time. The security of proposed protocols against possible kinds of active and passive attacks is proved using both informal method and BAN logic as a formal method.
- RFID

E-Health

Security

Authentication

Confidentiality

Availability

Traceability

Anonymity

- 2005 – 2007 **M.Sc. in Electrical Engineering** IUST
Title: Securing Documents using Hash Functions.
Supervisor: Prof. Majid Naderi
In MSc thesis, we introduced a new hash structure, called IMD. IMD is a general approach for strengthening standard iterative hash structure against multi-collision attack. We showed how to strengthen some vulnerable structures with this improvement. We proved that the modified structures are at least as strong against other attacks as the non-modified structures. In my thesis, we also have presented a new approach for distinguishing the iterative structure of hash function from a perfect hash function. Then we showed that some structures that previously seem to be strong against multi-collision attack, e.g. WPH, are vulnerable to this attack. We also showed that our proposed structure has a suitable security against this attack too.
- Hash Function

Collision Resistance

Random Oracle

Iterative Structure

Pre-image Resistance

Short Bio

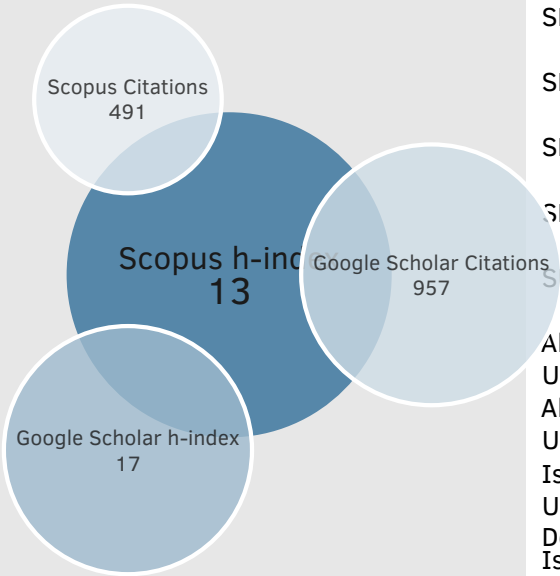
I finished my PhD on April 2012, in school of Electrical Engineering of Iran University of Science and Technology (IUST) where I did my MSc. and BSc. My research interests are in the field of protocols design, primitives design, lightweight cryptography, cryptanalysis etc.

I am currently working as an Associate Professor at Computer Engineering Department, Shahid Rajaei Teacher Training University, Tehran, Iran. Nowadays, beside previous research activities, I am working on the field of security protocols of telecommunications and the Internet of Things, symmetric cryptography primitives, and Searchable Encryption schemes. I welcome the collaboration with other researchers.

QR Code



Metrics



Undergraduate Study

2000 - 2004

B.Sc. in Electronics Engineering

IUST

Project Title: Design and Implementation of a Security System using Fingerprint Sensor.

Supervisor: Dr. Jamshid Fariborz. **Grade** Excellent

Fingerprint Sensor

Matlab

Security System

Biometric

Teaching Experience

Postgraduate Courses

SRTTU	Advanced Computer Networks 2017-2023	Fall
SRTTU	Advanced Networks Security 2017-2023	Spring
Alzahra University Tarbiat Modares University	Advanced Computer Networks 2017-2019 Applied Cryptography 2017-2019	Fall Fall

Undergraduate Courses

SRTTU	Assembly language and Microprocessors 2023	Spring
SRTTU	Computer Architecture 2022	Fall
SRTTU	Assembly language and Microprocessors 2022	Spring
SRTTU	Network Security 2018-2021	Spring
SRTTU	VHDL Digital Design 2015-2021	Spring
SRTTU	Computer Architecture 2015-2021	Fall
SRTTU	Computer Networks 2016-2018	Fall
SRTTU	Computer Architecture Lab 2014-2016	Fall
SRTTU	Microprocessors I 2014-2018	Fall
SRTTU	Microprocessors Lab 2014-2015	Fall
SRTTU	Cryptography 2016-2019	Spring
Alzahra University	Digital Logic Circuits Lab 2014-2015	Fall
Alzahra University	Engineering Probability and Statistics 2014-2015	Fall
Islamic Azad University Dezful Branch	Digital Circuits 2007-2009	Fall
Islamic Azad University Dezful Branch	Engineering Mathematics 2007-2009	Fall

Academic Supervision

2020–2023	Designing a secure consensus algorithm for use in blockchain 2020–2023	M.Sc.
2020–2022	Data clustering with privacy protection 2020–2022	M.Sc.
2018–2021	Improving Security of Data Mining from the Privacy Preserving Perspective 2018–2021	M.Sc.
2018–2020	Improving the Privacy Security of Telecare Medical Information Systems M.Sc. 2018–2020	
2018–2020	Improving Authentication Protocols in Internet of Vehicle (IoV) Networks M.Sc. 2018–2020	
2017–2021	Improving Security Protocols in Internet of Vehicles 2017–2020	M.Sc.
2017–2020	Security Improvement of IoT using Blockchain 2017–2020	M.Sc.
2017–2019	Security Improvement of Searchable Encryption Schemes in Databases M.Sc. 2017–2019	
2016–2018	Data Security Enhancing in Wireless Sensor Networks 2016–2018	M.Sc.
2016–2018	Improving Security Protocols in Internet of Things 2016–2018	M.Sc.
2014–2016	Security Analysis of SHA-3 Hash Function 2014–2016	M.Sc.
2014–2016	Improvement of Anti-Collision Protocols for RFID Systems Performance M.Sc. 2014–2016	

Skills

Programming:

MATLAB, C++, C, Pascal ● ● ● ● ●

Microprocessors Programming:

MIPS, x86, AVR, ARM ● ● ● ● ●

Hardware Programming:

Verilog, VHDL ● ● ● ● ●

Security Verification Tools:

AVISPA, Scyther, Proverif, Cryptoverif
● ● ● ● ●

CAD Tools:

Quartus, Modelsim, Proteus, Hspice, Pspice ● ● ● ● ●

Network Security Tools:

Wireshark, Metasploit, Nessus, Aircrack, Snort, Cain and Abel, Netcat ● ● ● ● ●

Network Simulation Tools:

OPNET ● ● ● ● ●

Memberships

Member of the Scientific Committee of the Iranian Society of Cryptology

Honours and Awards

May 2022	Award of Best Teacher	SRTTU,Iran
Dec 2021	Award of Research Excellence	SRTTU,Iran
Sep 2021	Award of Best M.Sc. thesis Supervision	ISCISC'18, Iran
Sep 2020	Award for Best Reviewer of ISCISC'17.	ISCISC'17, Iran
Sep 2019	Award for Best Reviewer of ISCISC'16.	ISCISC'16, Iran
Sep 2019	Award of Best M.Sc. thesis Supervision	ISCISC'16, Iran
Dec 2018	Award of Research Excellence	SRTTU,Iran
May 2017	Award of Best Teacher	SRTTU,Iran
Dec 2015	Award of Research Excellence	SRTTU,Iran

Invited Talks

May 2016	On the Security of RFID Systems	Shahid Beheshti University
	Gave a two hours lecture on RFID Security Protocols.	
Jan. 2012	Security Analysis of SNMP	CyberSpace Research Institute
	Gave a lecture on getting started in SNMP.	
Feb. 2012	Introduction to RFID Systems	Guilan University
	Gave a lecture on getting started in Security Analysis of RFID Protocols.	
Oct. 2010	Command and Control Networks' Simulation with OPNET	4th
	Conference of Iran's Scientific Society of (C4I), Sharif University of Technology	
	Gave a lecture on how simulate C4I networks in OPNET.	
Oct. 2009	Introduction to OPNET Software	3rd Conference of Iran's Scientific Society of (C4I), Malek Ashtar University of Technology
	Gave a lecture on getting started in OPNET.	

Review Duties

Journals:	IEEE Network	
	IEEE Transactions on Industrial Informatics	
	Concurrency and Computation: Practice and Experience	
	Journal of Information Systems and Telecommunication	
	Computer Networks	
	Computers and Electrical Engineering	
	Security and Communication Networks	
	IEEE Access	
	The Journal of Super Computing	
	IEEE Sensors Journal	
	Neural Computing and Applications (NCA)	
	International Journal of Information Security	
	Wireless Personal Communications	
	International Journal of Communication Systems	
	ISC International Journal of Information Security	
	Journal of Electronics Industries	
	Journal of Electrical and Computer Engineering	
	Innovations(JECEI)	
	Journal of Information Systems and Telecommunication	
Conferences:	ISCISC	2010-2022
	CSICC	2017-2021

Publications

Books

- M. Naderi and M. Safkhani. *Hash Function: Principles & Applications*. Iran University of Science & Technology Publications, 2008

Journals

- F. Pirmoradian, M. Safkhani, and S. M. Dakhilalian. Eccpws: An ecc-based protocol for wban systems. *Computer Networks*, page 109598, 2023
- F. G. Darbandeh and M. Safkhani. SAPWSN: A secure authentication protocol for wireless sensor networks. *Comput. Networks*, 220:109469, 2023
- C. Camara, P. Peris-Lopez, M. Safkhani, and N. Bagheri. Ecgsound for human identification. *Biomed. Signal Process. Control.*, 72(Part):103335, 2022
- S. Rostampour, N. Bagheri, Y. Bendavid, M. Safkhani, S. Kumari, and J. J. P. C. Rodrigues. An authentication protocol for next generation of constrained iot systems. *IEEE Internet Things J.*, 9(21):21493–21504, 2022
- M. Hosseinzadeh, R. Ali Naqvi, M. Safkhani, L. Tightiz, and R. Majid Mehmood. Secure authentication in the smart grid. *Mathematics*, 11(1):176, 2022
- M. Safkhani, N. Bagheri, S. Ali, M. Hussain Malik, O. Hassan Ahmed, M. Hosseinzadeh, and A. H. Mosavi. Improvement and cryptanalysis of a physically unclonable functions based authentication scheme for smart grids. *Mathematics*, 11(1):48, 2022
- M. R. Servati, M. Safkhani, S. Ali, M. H. Malik, O. H. Ahmed, M. Hosseinzadeh, and A. H. Mosavi. Cryptanalysis of two recent ultra-lightweight authentication protocols. *Mathematics*, 10(23):4611, 2022
- S. Zehtabchi, N. Daneshpour, and M. Safkhani. A new method for privacy preserving association rule mining using homomorphic encryption with a secure communication protocol. *Wireless Networks*, pages 1–16, 2022
- J. Alizadeh, M. Safkhani, and A. Allahdadi. Isaka: Improved secure authentication and key agreement protocol for wban. *Wireless Personal Communications*, 126(4):2911–2935, 2022
- M. Akbari Azimian, N. Daneshpour, and M. Safkhani. Privacy preserving naïve bayes classification using bit-string encryption. *Journal of Soft Computing and Information Technology*, 11(1):73–88, 2022
- S. Rostampour, N. Bagheri, Y. Bendavid, M. Safkhani, S. Kumari, and J. J. Rodrigues. An authentication protocol for next generation of constrained iot systems. *IEEE Internet of Things Journal*, 9(21):21493–21504, 2022
- M. Safkhani, S. Rostampour, Y. Bendavid, S. Sadeghi, and N. Bagheri. Improving RFID/IoT-based generalized ultra-lightweight mutual authentication protocols. *Journal of Information Security and Applications*, 67:103194, 2022
- M. Safkhani, S. Kumari, M. Shojafar, and S. Kumar. An authentication and key agreement scheme for smart grid. *Peer-to-Peer Networking and Applications*, pages 1–22, 2022
- C. Camara, P. Peris-Lopez, M. Safkhani, and N. Bagheri. Ecgsound for human identification. *Biomed. Signal Process. Control.*, 72(Part):103335, 2022
- J. Lansky, A. M. Rahmani, S. Ali, N. Bagheri, M. Safkhani, O. Hassan Ahmed, and M. Hosseinzadeh. Bcmecc: A lightweight blockchain-based authentication and key agreement protocol for internet of things. *Mathematics*, 9(24):3241, 2021
- F. Moazami and M. Safkhani. Tbgodp⁺: improvement of tbgodp, a time bound group ownership delegation protocol. *Journal of Ambient Intelligence and Humanized Computing*, pages 1–20, 2021
- A. M. Rahmani, M. Mohammadi, J. Lansky, S. Mildeová, M. Safkhani, S. Kumari, S. H. T. Karim, and M. Hosseinzadeh. AMAPG: advanced mobile authentication protocol for GLOMONET. *IEEE Access*, 9:88256–88271, 2021
- A. M. Rahmani, M. Mohammadi, S. Rashidi, J. Lansky, S. Mildeová, M. Safkhani, S. Kumari, and M. Hosseinzadeh. Questioning the security of three recent authentication and key agreement protocols. *IEEE Access*, 9:98204–98217, 2021
- F. Nikkhah and M. Safkhani. LAPCHS: A lightweight authentication protocol for cloud-based health-care systems. *Comput. Networks*, 187:107833, 2021
- M. Safkhani, C. Camara, P. Peris-Lopez, and N. Bagheri. RSEAP2: an enhanced version of rseap, an RFID based authentication protocol for vehicular cloud computing. *Veh. Commun.*, 28:100311, 2021

- M. Zamani, M. Safkhani, N. Daneshpour, and A. Abbasian. A new searchable encryption scheme with integrity preservation property. *Wirel. Pers. Commun.*, 116(4):3119–3142, 2021
- M. Hosseinzadeh, J. Lansky, A. M. Rahmani, C. Trinh, M. Safkhani, N. Bagheri, and B. Huynh. A new strong adversary model for RFID authentication protocols. *IEEE Access*, 8:125029–125045, 2020
- C. Trinh, B. Huynh, J. Lansky, S. Mildeová, M. Safkhani, N. Bagheri, S. Kumari, and M. Hosseinzadeh. A novel lightweight block cipher-based mutual authentication protocol for constrained environments. *IEEE Access*, 8:165536–165550, 2020
- M. Safkhani, N. Bagheri, S. Kumari, H. Tavakoli, S. Kumar, and J. Chen. RESEAP: an ecc-based authentication and key agreement scheme for iot applications. *IEEE Access*, 8:200851–200862, 2020
- M. Safkhani, S. Rostampour, Y. Bendavid, and N. Bagheri. Iot in medical & pharmaceutical: Designing lightweight RFID security protocols for ensuring supply chain integrity. *Comput. Networks*, 181:107558, 2020
- S. Rostampour, M. Safkhani, Y. Bendavid, and N. Bagheri. Eccbap: A secure ecc-based authentication protocol for iot edge devices. *Pervasive Mob. Comput.*, 67:101194, 2020
- M. Yavari, M. Safkhani, S. Kumari, S. Kumar, and C. Chen. An improved blockchain-based authentication protocol for iot network management. *Secur. Commun. Networks*, 2020:8836214:1–8836214:16, 2020
- F. Moazami and M. Safkhani. SEOTP: a new secure and efficient ownership transfer protocol based on quadric residue and homomorphic encryption. *Wirel. Networks*, 26(7):5285–5306, 2020
- F. G. Darbandeh and M. Safkhani. A new lightweight user authentication and key agreement scheme for WSN. *Wirel. Pers. Commun.*, 114(4):3247–3269, 2020
- A. Abbasian and M. Safkhani. CNCAA: A new anti-collision algorithm using both collided and non-collided parts of information. *Comput. Networks*, 172:107159, 2020
- M. Safkhani and A. V. Vasilakos. A new secure authentication protocol for telecare medicine information system and smart campus. *IEEE Access*, 7:23514–23526, 2019
- M. Safkhani. Full secret disclosure attack against an epc-c1 g2 compliant authentication protocol. *Journal of Computing and Security*, 6(1):13–23, 2019
- S. Hosiny Nezhad, M. Safkhani, and N. Bagheri. Relaxed differential fault analysis of sha-3. *The ISC International Journal of Information Security*, 11(2):129–143, 2019
- Y. Bendavid, N. Bagheri, M. Safkhani, and S. Rostampour. Iot device security: Challenging "a lightweight RFID mutual authentication protocol based on physical unclonable function". *Sensors*, 18(12):4444, 2018
- N. Bagheri, M. Safkhani, M. E. Namin, and S. Rostampour. An improved low-cost yoking proof protocol based on kazahaya's flaws. *J. Supercomput.*, 74(5):1934–1948, 2018
- M. Safkhani and M. Shariat. Implementation of secret disclosure attack against two iot lightweight authentication protocols. *J. Supercomput.*, 74(11):6220–6235, 2018
- M. Safkhani, N. Bagheri, and M. Shariat. On the security of rotation operation based ultra-lightweight authentication protocols for RFID systems. *Future Internet*, 10(9):82, 2018
- A. Abbasian and M. Safkhani. A new EPC-C1G2 based anti-collision algorithm to address tags'starvation in RFID systems. *NASHRIYYAH-I MUHANDISI-I BARQ VA MUHANDISI-I KAMPYUTAR-I*, 2018
- M. Safkhani. Cryptanalysis of R2AP an ultralightweight authentication protocol for RFID. *Journal of Electrical and Computer Engineering Innovations*, 6(1):107–114, 2018
- M. Safkhani and N. Bagheri. Passive secret disclosure attack on an ultralightweight authentication protocol for internet of things. *J. Supercomput.*, 73(8):3579–3585, 2017
- M. Safkhani, M. Hosseinzadeh, M. E. Namin, S. Rostampour, and N. Bagheri. On the (im)possibility of receiving security beyond 2 l using an l-bit PRNG. *Wirel. Pers. Commun.*, 92(4):1591–1597, 2017
- M. Safkhani and A. Abbasian. On the security of the revised SRP+ RFID authentication protocol. *Electronics Industries*, 8(3):145–149, 2017
- M. Safkhani and M. Arghavani. A survey of cube, differential fault analysis attacks and linear structures on keccak hash function (sha-3). *Biannual Journal Monadi for Cyberspace Security (AFTA)*, 5(2):3–14, 2017
- M. Safkhani and N. Bagheri. A note on the security of two improved RFID protocols. *ISC Int. J. Inf. Secur.*, 8(2):155–160, 2016

- N. Bagheri, F. Baghernejhad, and M. Safkhani. On the designing of EPC C1 G2 authentication protocol using AKARI-1 and AKARI-2 prngs. *Inf. Technol. Control.*, 44(1):41–53, 2015
- M. Safkhani, N. Bagheri, and A. Mahani. On the security of RFID anti-counting security protocol (ACSP). *J. Comput. Appl. Math.*, 259:512–521, 2014
- M. Safkhani, P. Peris-Lopez, J. C. H. Castro, and N. Bagheri. Cryptanalysis of the cho et al. protocol: A hash-based RFID tag mutual authentication protocol. *J. Comput. Appl. Math.*, 259:571–577, 2014
- N. Bagheri, M. Safkhani, and M. Naderi. Cryptanalysis of a new EPC class-1 generation-2 standard compliant RFID protocol. *Neural Comput. Appl.*, 24(3-4):799–805, 2014
- N. Bagheri, M. Safkhani, P. Peris-Lopez, and J. E. Tapiador. Weaknesses in a new ultralightweight RFID authentication protocol with permutation - RAPP. *Secur. Commun. Networks*, 7(6):945–949, 2014
- M. Safkhani, N. Bagheri, and M. Naderi. Strengthening the security of EPC C-1 G-2 RFID standard. *Wirel. Pers. Commun.*, 72(2):1295–1308, 2013
- M. Safkhani and N. Bagheri. For an EPC-C1 G2 RFID compliant protocol, CRC with concatenation : No; PRNG with concatenation : Yes. *IACR Cryptol. ePrint Arch.*, page 490, 2013
- M. Safkhani, N. Bagheri, and M. Naderi. On the designing of a tamper resistant prescription RFID access control system. *J. Medical Syst.*, 36(6):3995–4004, 2012

Conferences

- M. Shariat and M. Safkhani. How the control over smart meters is lost in the yan et al. lightweight aka scheme for smart grids. In *2017 9th International Conference on Information and Knowledge Technology (IKT)*, pages 82–84. IEEE, 2017
- H. Jannati, N. Bagheri, and M. Safkhani. Analysis of a distance bounding protocol for verifying the proximity of two-hop neighbors. In *14th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology, ISCISC 2017, Shiraz, Iran, September 6-7, 2017*, pages 31–36. IEEE, 2017
- M. Safkhani, H. Jannati, and N. Bagheri. Security analysis of niu et al. authentication and ownership management protocol. In G. P. Hancke and K. Markantonakis, editors, *Radio Frequency Identification and IoT Security - 12th International Workshop, RFIDSec 2016, Hong Kong, China, November 30 - December 2, 2016, Revised Selected Papers*, volume 10155 of *Lecture Notes in Computer Science*, pages 3–16. Springer, 2016
- S. F. Aghili, N. Bagheri, P. Gauravaram, M. Safkhani, and S. K. Sanadhya. On the security of two RFID mutual authentication protocols. In M. Hutter and J. Schmidt, editors, *Radio Frequency Identification - Security and Privacy Issues 9th International Workshop, RFIDsec 2013, Graz, Austria, July 9-11, 2013, Revised Selected Papers*, volume 8262 of *Lecture Notes in Computer Science*, pages 86–99. Springer, 2013
- N. Bagheri, P. Gauravaram, M. Safkhani, and S. K. Sanadhya. Desynchronization and traceability attacks on RIPTA-DA protocol. In M. Hutter and J. Schmidt, editors, *Radio Frequency Identification - Security and Privacy Issues 9th International Workshop, RFIDsec 2013, Graz, Austria, July 9-11, 2013, Revised Selected Papers*, volume 8262 of *Lecture Notes in Computer Science*, pages 57–68. Springer, 2013
- M. Safkhani, P. Peris-Lopez, N. Bagheri, M. Naderi, and J. C. H. Castro. On the security of tan et al. serverless RFID authentication and search protocols. In J. Hoepman and I. Verbauwhede, editors, *Radio Frequency Identification. Security and Privacy Issues - 8th International Workshop, RFIDSec 2012, Nijmegen, The Netherlands, July 2-3, 2012, Revised Selected Papers*, volume 7739 of *Lecture Notes in Computer Science*, pages 1–19. Springer, 2012
- M. Safkhani, N. Bagheri, S. K. Sanadhya, M. Naderi, and H. Behnam. On the security of mutual authentication protocols for RFID systems: The case of wei et al.'s protocol. In J. García-Alfaro, G. Navarro-Arribas, N. Cuppens-Boulahia, and S. D. C. di Vimercati, editors, *Data Privacy Management and Autonomous Spontaneous Security - 6th International Workshop, DPM 2011, and 4th International Workshop, SETOP 2011, Leuven, Belgium, September 15-16, 2011, Revised Selected Papers*, volume 7122 of *Lecture Notes in Computer Science*, pages 90–103. Springer, 2011
- M. Safkhani, N. Bagheri, and M. Naderi. Vulnerabilities in a new RFID access control protocol. In *6th International Conference for Internet Technology and Secured Transactions, ICITST 2011, Abu Dhabi, UAE, December 11-14, 2011*, pages 500–503. IEEE, 2011
- M. Safkhani, N. Bagheri, M. Naderi, and S. K. Sanadhya. Security analysis of Imap⁺⁺, an RFID authentication protocol. In *6th International Conference for Internet Technology and Secured Transactions, ICITST 2011, Abu Dhabi, UAE, December 11-14, 2011*, pages 689–694. IEEE, 2011

- M. Safkhani, N. Bagheri, M. Naderi, Y. Luo, and Q. Chai. Tag impersonation attack on two RFID mutual authentication protocols. In *Sixth International Conference on Availability, Reliability and Security, ARES 2011, Vienna, Austria, August 22-26, 2011*, pages 581–584. IEEE Computer Society, 2011
- A. Kumar, S. K. Sanadhya, P. Gauravaram, M. Safkhani, and M. Naderi. Cryptanalysis of tav-128 hash function. In G. Gong and K. C. Gupta, editors, *Progress in Cryptology - INDOCRYPT 2010 - 11th International Conference on Cryptology in India, Hyderabad, India, December 12-15, 2010. Proceedings*, volume 6498 of *Lecture Notes in Computer Science*, pages 118–130. Springer, 2010